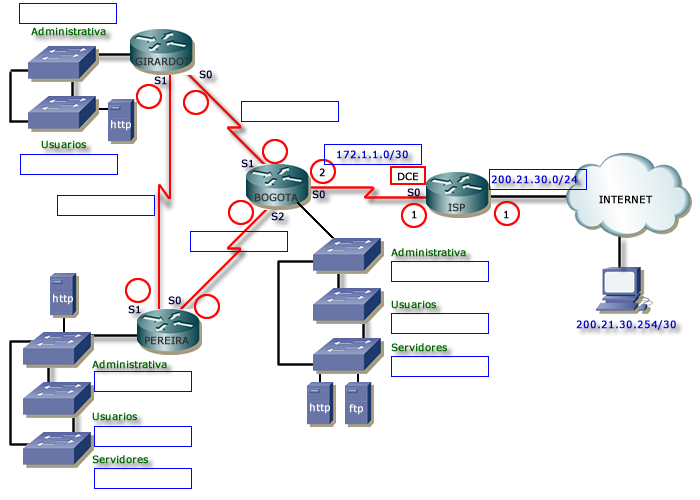
# descripción

La Universidad está interesada en implementar su red de datos. La sede principal está ubicada en Bogotá, y, cuenta con tres redes LAN: una para los empleados de Administrativa, la segunda para los usuarios que están compuestos por los docentes y los estudiantes y la tercera para ubicar los servidores necesarios. Las necesidades de la sede de Pereira son similares, mientras que en Girardot sólo se requieren dos redes LAN, tal como se ilustra en la topología lógica de la siguiente gráfica.



La tarea consiste en diseñar, implementar y documentar completamente la red de la Universidad. Además del informe formal, la Universidad desea ver un prototipo de la red construida en un simulador, antes de su implementación total, para confirmar que satisface sus necesidades.

# Fase 1 - Esquema de direccionamiento.

La Universidad solicita utilizar para su direccionamiento interno subredes y VLSM, con direcciones privadas IPV4 de acuerdo con el RFC 1918 y con las siguientes condiciones:

## 1.1 REQUISITOS DE HOST

Para calcular el número de hosts de cada una las redes, se utilizará como base la variable **X** que será el resultado de sumar los tres últimos dígitos del documento de identidad de cada uno de los estudiantes que componen el grupo, multiplicado por diez (10). En caso de que la variable **X** resulte inferior a 3000, los estudiantes solicitarán al profesor la asignación de un valor para dicha variable.

|  |  |
| --- | --- |
| **NOMBRES Y APELLIDOS** | **ÚLTIMOS TRES DÍGITOS DOC. ID** |
| Cesar Chávez | 693 |
| Mauricio García | 522 |
| Sebastian Castillo Castillo | 544 |
| Brayan Burgos Zambrano | 496 |
| Zamir Eduardo Patarroyo Granados | 554 |
| **SUMA \* 10** | 28.090 |

La siguiente tabla muestra los requisitos de host para cada una de las redes con base en la variable **X**

|  |  |  |
| --- | --- | --- |
| **RED** | **FACTOR** | **TOTAL HOST REQUERIDOS** |
| **Administrativa – Bogotá** | **2X** | 56.180 |
| **Usuarios – Bogotá** | **X** | 28.090 |
| **Servidores - Bogotá** | **X/500** | 56 |
| **Administrativa – Pereira** | **X/2** | 14.045 |
| **Usuarios – Pereira** | **X/4** | 7.022 |
| **Servidores - Pereira** | **X/1000** | 28 |
| **Administrativa – Girardot** | **X/6** | 4.681 |
| **Usuarios – Giradot** | **X/12** | 2.340 |
| **Enlace Bogotá-Pereira** | **N/A** | 2 |
| **Enlace Bogotá-Girardot** | **N/A** | 2 |
| **Enlace Girardot-Pereira** | **N/A** | 2 |

## 1.2 REQUISITOS DE DIRECCIONAMIENTO

Con base en los cálculos de requisitos de host del punto anterior, se debe escoger una dirección de red PRIVADA apropiada para satisfacer las necesidades de la Universidad.

|  |  |  |
| --- | --- | --- |
| **DIRECCIÓN DE RED ESCOGIDA** | **CLASE** | **MÁSCARA DE SUBRED** |
| **10.0.0.0** | **A** | 255.0.0.0 |

* Usar la subred 172.1.1.0/30 para conectar Bogotá con el ISP.
* Usar la subred 200.21.30.0/24 para simular Internet.

Se debe crear una tabla en la que figuren todas las subredes posibles que satisfagan los requisitos de la Universidad, utilizando un diseño VLSM. Las subredes que no se utilizarán deben estar claramente identificadas en la tabla como segmentos libres.

De acuerdo con lo anterior y con el diagrama lógico suministrado se tienen las siguientes redes:

|  |  |  |
| --- | --- | --- |
| **NOMBRE DE LA RED** | **HOST REQUERIDOS** | **DESCRIPCIÓN** |
| **Administrativa – Bogotá** | 56.180 |  |
| **Usuarios – Bogotá** | 28.090 |  |
| **Servidores - Bogotá** | 56 |  |
| **Administrativa – Pereira** | 14.045 |  |
| **Usuarios – Pereira** | 7.022 |  |
| **Servidores - Pereira** | 28 |  |
| **Administrativa – Girardot** | 4.681 |  |
| **Usuarios – Giradot** | 2.340 |  |
| **Enlace Bogotá-Pereira** | **2** |  |
| **Enlace Bogotá-Girardot** | **2** |  |
| **Enlace Girardot-Pereira** | **2** |  |

Se dispone de la dirección 10 . 0. \_0 . 0 de red clase A (la escogida por el grupo), con la cual se deben suplir las necesidades de direccionamiento IP, utilizando para ello VLSM.

Se debe hacer aquí una explicación detallada del proceso para hacer la distribución y asignación de direcciones IP, utilizando las técnicas de VLSM, incluyendo un pequeño resumen del marco teórico de IP y VLSM.

**Se deben incluir todos los cálculos realizados**.

## 1.3 ESQUEMA DIRECCIONAMIENTO IP.

Diligenciar la siguiente tabla de acuerdo con los cálculos y resultados de VLSM (Se deben incluir todos los segmentos de red libres):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nombre** | **RED**  **Nº** | **HOSTS**  **REQUERIDOS**  **(ÚTILES)** | **DIRECCIÓN DE RED** | **DIRECIÓN BROADCAST** | **MÁSCARA SUBRED** | **HOST UTILIZABLES** |
| **Admin-Bogotá** | **1** | **56.180** | **10.0.0.0** | **10.0.255.255** | **255.255.0.0** | **65.534** |
| **Libre-Bogotá** | **2** | **54.000** | **10.1.0.0** | **10.1.255.255** | **255.255.0.0** | **65.534** |
| **Usuario-Bogotá** | **3** | **28.090** | **10.2.0.0** | **10.2.127.255** | **255.255.128.0** | **32.766** |
| **Admin-Pereira** | **4** | **14.045** | **10.2.128.0** | **10.2.128.255** | **255.255.128.0** | **32.766** |
| **Libre-Pereira** | **5** | **10.000** | **10.3.0.0** | **10.3.63.255** | **255.255.192.0** | **16.382** |
| **Usuario-Pereira** | **6** | **7.022** | **10.3.64.0** | **10.3.127.255** | **255.255.192.0** | **16.382** |
| **Admin-Girardot** | **5** | **4.681** | **10.3.128.0** | **10.3.159.255** | **255.255.224.0** | **8.192** |
| **Usuarios-Girardot** | **7** | **2.340** | **10.3.160.0** | **10.3.175.255** | **255.255.240.0** | **4.096** |
| **Libre-Girardot** | **8** | **2.000** | **10.3.176.0** | **10.3.191.255** | **255.255.240.0** | **4.096** |
| **Servidores-Bogotá** | **9** | **56** | **10.3.192.0** | **10.3.191.127** | **255.255.255.128** | **62** |
| **Servidores-Pereira** | **10** | **28** | **10.3.192.128** | **10.3.191.191** | **255.255.255.192** | **62** |
| GIRARDOT-BOGOTA | 11 | 2 | 37.0.0.0 | 37.0.0.3 | 255.255.255.252 | 2 |
| GIRARDOT-PEREIRA | 12 | 2 | 37.0.0.4 | 37.0.0.7 | 255.255.255.252 | 2 |
| PEREIRA-BOGOTA | 13 | 2 | 37.0.0.8 | 37.0.0.11 | 255.255.255.252 | 2 |
|  |  |  |  |  |  |  |

## 1.4 DIAGRAMA LÓGICO

Se debe presentar el diagrama lógico indicando todos datos pertinentes.

## 

## 1.5 DESCRIPCIÓN DE ROUTERS

Para cada ubicación, incluida Internet, se requiere otro conjunto de tablas. Estas tablas sirven de ayuda para las actividades de diseño y desarrollo y se usan al configurar los routers. Se debe crear una tabla separada para cada router, con las siguientes columnas:

### Ubicación: Bogotá

**Nombre del router: ISP**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TIPO**  **Y Nº DE**  **INTERFAZ** | **DCE**  **DTE** | **CLOCK**  **RATE** | **NOMBRE**  **RED** | **DIRECCIÓN**  **RED** | **DIR IP**  **INTERFAZ** | **MÁSCARA**  **SUBRED** |
| 2/0 | DTE | N/A | ISP-BOGOTA | 172.1.1.0 | 172.1.1.2 | 255.255.255.252 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### Ubicación: Bogotá

**Nombre del router: BOGOTA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TIPO**  **Y Nº DE**  **INTERFAZ** | **DCE**  **DTE** | **CLOCK**  **RATE** | **NOMBRE**  **RED** | **DIRECCIÓN**  **RED** | **DIR IP**  **INTERFAZ** | **MÁSCARA**  **SUBRED** |
| Serial2/0 | DCE | 64000 | BOGOTA-ISP | 172.1.1.0 | 172.1.1.1 | 255.255.255.252 |
| Serial 3/0 | DCE | 64000 | BOGOTA-GIRARDOT | 37.0.0.0 | 37.0.0.2 | 255.255.255.252 |
| Serial 6/0 | DCE | 64000 | BOGOTA-PEREIRA | 37.0.0.8 | 37.0.0.10 | 255.255.255.252 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### Ubicación: Girardot

**Nombre del router: Girardot**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TIPO**  **Y Nº DE**  **INTERFAZ** | **DCE**  **DTE** | **CLOCK**  **RATE** | **NOMBRE**  **RED** | **DIRECCIÓN**  **RED** | **DIR IP**  **INTERFAZ** | **MÁSCARA**  **SUBRED** |
| Serial2/0 | DTE | N/A | GIRARDOT-BOGOTA | 37.0.0.0 | 37.0.0.1 | 255.255.255.252 |
| Serial 3/0 | DTE | N/A | GIRARDOT-PEREIRA | 37.0.0.4 | 37.0.0.5 | 255.255.255.252 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### Ubicación: Pereira

**Nombre del router: Pereira**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TIPO**  **Y Nº DE**  **INTERFAZ** | **DCE**  **DTE** | **CLOCK**  **RATE** | **NOMBRE**  **RED** | **DIRECCIÓN**  **RED** | **DIR IP**  **INTERFAZ** | **MÁSCARA**  **SUBRED** |
| Serial3/0 | DCE | 64000 | PEREIRA-GIRARDOT | 37.0.0.4 | 37.0.0.6 | 255.255.255.252 |
| Serial 3/0 | DTE | N/A | GIRARDOT-PEREIRA | 37.0.0.4 | 37.0.0.5 | 255.255.255.252 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# FASE 2 – ENRUTAMIENTO Y CONFIGURACIÓN BÁSICA DE ROUTERS

La Universidad desea que se recomiende un protocolo de enrutamiento para la red, que sea el más adecuado para las condiciones que se tienen. Las alternativas y propiedades del posible protocolo de enrutamiento se deben identificar y describir, haciendo un resumen de las principales características, ventajas y desventajas de los protocolos conocidos, así como un marco teórico de enrutamiento. Posteriormente se hará un análisis y se recomendará el protocolo a ser utilizado. El resultado de los análisis de cada uno de los protocolos, se debe resumir en una tabla asignando un valor numérico o cualitativo a cada una de las propiedades, por ejemplo, 0 a 5. Se realiza luego una recomendación y la matriz de decisiones se presenta a la Universidad.

**Marco teórico de enrutamiento y protocolos de enrutamiento**

El enrutamiento es el proceso mediante el cual los routers deciden cómo enviar paquetes de datos desde un origen hacia un destino. Esto se realiza mediante tablas de enrutamiento, que contienen información sobre las rutas que los paquetes deben seguir.

1. **Tipos de protocolos de enrutamiento**
2. RIP (Routing Information Protocol):

* Tipo: Protocolo de enrutamiento por vector de distancia.
* Distancia administrativa:120.
* Actualización de la tabla: Cada 30 segundos.
* Límite de saltos: 15 saltos.
* Ventajas: Fácil de configurar, ligero.
* Desventajas: No es escalable para redes grandes, lento en convergencia.

1. OSPF (Open Shortest Path First):

* Tipo: Protocolo de enrutamiento por estado de enlace.
* Distancia administrativa: 110.
* Convergencia: Rápida.
* Ventajas: Escalable, adecuado para redes grandes y jerárquicas, rápida convergencia.
* Desventajas: Complejo de configurar, requiere más recursos de CPU y memoria.

1. EIGRP (Enhanced Interior Gateway Routing Protocol):

* Tipo: Protocolo híbrido (vector de distancia con características de estado enlace)
* Distancia administrativa: 90 (rutas internas).
* Convergencia: Rápida.
* Ventajas: Equilibrio entre simplicidad y escalabilidad, buena convergencia.
* Desventajas: Propietario de Cisco (limitado si usas routers no Cisco), complejo para configurar.

1. **Análisis comparativo de los protocolos**

Podemos evaluar los protocolos usando una matriz de decisión con diferentes criterios, evaluando de 0 a 5, donde 5 es la máxima calificación:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Protocolo** | **Facilidad de configuración** | **Escalabilidad** | **Convergencia** | **Consumo de recursos** | **Seguridad** |
| RIPv2 | 5 | 3 | 2 | 5 | 3 |
| OSPF | 3 | 5 | 5 | 3 | 4 |
| EIGRP | 4 | 4 | 5 | 4 | 4 |

Recomendaciones:

* Si la red es grande y necesita escalabilidad y rapidez, (OSPF o EIGRP) serían las mejores opciones.
* Para una red mediana o pequeña, donde la simplicidad es clave, RIP puede ser suficiente, aunque con limitaciones.

Una vez analizados los protocoles el comité de compañeros evaluó que el protocolo más adecuado para garantizar la interoperabilidad y eficiencia de la red es el de Ripv2.

1. **Marco teórico sobre RIPv2**

RIPv2 (Routing Information Protocol version 2) es un protocolo de enrutamiento por vector de distancia utilizado en redes pequeñas y medianas. Soporta más funcionalidades, como el enrutamiento classless y el uso de máscaras de subred (VLSM), lo que lo hace más flexible.

Características principales de RIPv2:

* Distancia administrativa: 120.
* Algoritmo: Vector de distancia (utiliza la métrica de saltos o "hops" para determinar la mejor ruta).
* Límite de saltos: 15 saltos (16 es considerado inalcanzable).
* Actualización de la tabla de enrutamiento: Cada 30 segundos.
* Soporte para VLSM (Variable Length Subnet Masking): Eficiente en redes que requieren subredes.
* Autenticación: RIPv2 soporta autenticación.
* Desventajas: Convergencia lenta y poco escalable para redes muy grandes.
* Ventajas de RIPv2:

1. Facilidad de configuración: Es simple y fácil de entender, por lo que es ideal para administradores con poca experiencia en enrutamiento.
2. Compatibilidad: RIPv2 es compatible con pequeñas redes y tiene soporte para el uso de máscaras de subred variables (VLSM).

3. Bajo consumo de recursos: Comparado con OSPF o EIGRP, RIPv2 consume menos recursos de CPU y memoria.

## 2.1 CONDICIONES DE ENRUTAMIENTO

Se debe planificar el enrutamiento utilizando el protocolo recomendado, reforzado con rutas estáticas de backup. En el router Bogotá se debe implementar lo necesario para que la ruta de salida a Internet sea redistribuida.

1. **Configuración del protocolo RIPv2**

En cada router, activaremos RIPv2, especificando las redes involucradas.

1. **Rutas estáticas de backup**

Añadiremos rutas estáticas que servirán como respaldo si las rutas dinámicas fallan.

1. **Redistribución de la ruta de salida a Internet**

En el router Bogotá, configuraremos una redistribución para que otras rutas puedan aprender cómo salir a Internet.

* Configuración de RIPv2 en los routers: Para que todos los routers compartan la información de enrutamiento, se configura RIPv2 en cada uno de ellos.
* Habilitar RIP en el router Bogotá

enable

configure terminal

router rip

version 2

network 192.168.1.0 # Incluir redes conectadas a cada router

network 10.0.0.0 # Incluir redes conectadas a cada router

no auto-summary # Deshabilita la suma automática de redes

exit

* Configuración de rutas estáticas de backup: Las rutas estáticas son necesarias para que puedas tener una vía alternativa si RIPv2 falla en proporcionar una ruta.
* Configuración de una ruta estática en el router Bogotá

ip route 192.168.2.0 255.255.255.0 10.0.0.2 Ruta estática de respaldo

ip route 192.168.3.0 255.255.255.0 10.0.0.3 Respaldo

192.168.2.0 y 192.168.3.0 son las redes destino.

10.0.0.2 y 10.0.0.3 son las direcciones IP del siguiente salto.

1. **Redistribución de la ruta de salida a Internet en el router Bogotá**

Redistribuir la ruta de salida a Internet significa permitir que el resto de la red conozca cómo alcanzar la red de Internet a través del router Bogotá.

* Configurar una ruta estática predeterminada hacia la red de Internet
* Ruta predeterminada para la salida a Internet en el router Bogotá

ip route 0.0.0.0 0.0.0.0 200.100.50.1

Aquí 200.100.50.1 es la dirección IP de la puerta de enlace o router que conecta con Internet.

* Redistribución de la ruta estática en RIPv2

router rip

default-information originate #Redistribuir la ruta predeterminada hacia Intern

Con este comando, el router Bogotá propagará la ruta predeterminada a otros routers en la red, permitiéndoles aprender cómo salir a Internet.

1. **Configuraciones adicionales (de acuerdo con los requerimientos)**

* Contraseñas y seguridad básica:

enable secret Cisco123

line console 0

password Cisco123

login

line vty 0 4

password Cisco123

login

service password-encryption

* Ajustes para el router:

no ip domain-lookup # Deshabilitar la búsqueda DNS

exec-timeout 5 0 # Tiempo de espera de 5 minutos para consola y vty

banner motd # Bienvenido al Router Bogota #

logging synchronous # Sincronización de mensajes de consola

history size 200 # Habilitar historial de comandos

## 2.2 CONFIGURACIÓN BÁSICA DE ROUTERS

Se debe garantizar la conectividad entre todos los dispositivos, así como, la salida a Internet. La configuración de los dispositivos se entregará en archivos de texto plano capturados: un archivo para cada router. Se debe incluir dentro de la configuración, además de los comandos propios de enrutamiento, los siguientes:

* Contraseña de acceso a consola, terminales virtuales y modo privilegiado.
* Servicio de encripción de passwords
* Deshabilitar la búsqueda DNS
* Configurar tiempo de espera de 5 minutos para consola y vty
* Mensaje del día
* Descripción de interfaces
* Sincronización de mensajes de consola
* Habilitar historial de comandos para que guarde los últimos 200

La implementación del modelo se realizará en un simulador y el modelo funcional será entregado como evidencia.

**Nota**: Los comandos que no estén disponibles en el simulador, deberán ser agregados manualmente a los archivos de configuración.

**Configuración básica para RIPv2**

* Router Bogotá: Configuración básica del router Bogotá con RIPv2

enable

configure terminal

hostname RouterBogota

* Configuración de contraseñas

enable secret Cisco123

line console 0

password Cisco123

login

line vty 0 4

password Cisco123

login

service password-encryption

* Configuración de interfaces

interface GigabitEthernet0/0

description Conexión a la LAN

ip address 192.168.1.1 255.255.255.0

no shutdown

interface GigabitEthernet0/1

description Conexión a Internet

ip address 200.100.50.1 255.255.255.252

no shutdown

* Configuración de RIPv2

router rip

version 2

network 192.168.1.0

network 200.100.50.0

no auto-summary

* Configuración de ruta estática para salida a Internet

ip route 0.0.0.0 0.0.0.0 200.100.50.2

* Configuración adicional

no ip domain-lookup

exec-timeout 5 0

banner motd # Bienvenido al Router Bogota #

logging synchronous

history size 200

end

write memory

# FASE 3 – CONMUTACIÓN

La Universidad en la actualidad cuenta con el número de switches en cada sede mostrados en el diagrama de la topología (Bogotá 3, Pereira 3 y Giradot 2). Se creé que en el futuro el número de estos dispositivos crecerá, por lo que se solicita designar un segmento de red para cada ciudad, con el propósito de asignar direcciones a cada switch y de esta manera facilitar su administración remota. A continuación se muestra la cantidad de dispositivos. El factor **X** corresponde al último dígito del documento de identidad del último participante del grupo:

* Bogotá: 3(4)
* Pereira: 3(4)
* Girardot: 2(4)

De las direcciones de red libres, seleccionar 3 nuevas redes que se utilizarán para asignarlas a los switches de cada una de las sedes.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RED** | **HOSTS**  **REQUERIDOS**  **(ÚTILES)** | **DIRECCIÓN DE RED** | **DIRECIÓN BROADCAST** | **MÁSCARA SUBRED** | **HOST UTILIZABLES** |
| **Switches**  **Bogotá** | 12 |  |  |  |  |
| **Switches Pereira** | 12 |  |  |  |  |
| **Switches Girardot** | 8 |  |  |  |  |

## 3.1 CONFIGURACIÓN BÁSICA DE SWITCHES

La configuración de los dispositivos se entregará en archivos de texto plano capturados: un archivo para cada switch. Se debe incluir dentro de la configuración, además de los comandos propios de conmutación, los siguientes:

* Contraseña de acceso a consola, terminales virtuales y modo privilegiado.
* Servicio de encriptación de contraseñas
* Deshabilitar la búsqueda DNS
* Configurar tiempo de espera de 5 minutos para consola y terminales vty
* Mensaje del día
* Sincronización de mensajes de consola
* Habilitar historial de comandos para que guarde los últimos 200

## 3.2 CONFIGURACIÓN DE LANs VIRTUALES

Teniendo en cuenta que habrá personal de cada una de las sedes ubicado en los diferentes pisos de la edificación, se deben configurar las VLANs necesarias en cada uno de los switches: Administrativa, Usuarios y Servidores. La universidad desea que se utilice VTP con el fin de facilitar la administración de las VLANs, para lo cual, se configurará uno de los switches como servidor y los demás como clientes. Se debe suministrar la siguiente información relacionada con la configuración de VTP:

**Configuración VTP**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SEDE** | **SWITCH**  **SERVIDOR** | **SWITCHES CLIENTE** | **DOMINIO VTP** | **VERSIÓN VTP** | **CONTRASEÑA VTP** |
| **Bogotá** |  |  |  |  |  |
| **Pereira** |  |  |  |  |  |
| **Girardot** |  |  |  |  |  |

## 3.3 REDUNDANCIA FÍSICA

La Universidad desea que las redes LAN sean diseñadas con cierta seguridad, utilizando para ello redundancia de enlaces y el protocolo STP. Se debe asegurar, mediante la configuración de STP, que el switch ubicado en el último piso de cada edificación sea el switch raíz. Se debe incluir una explicación detallada de las tareas de configuración para lograr esto.

## 3.4 DETALLES DE CONFIGURACIÓN DE SWITCHES

En el modelo de simulación, se deben configurar al menos dos dispositivos en cada VLAN, indicando en una tabla todos los detalles de configuración necesarios, tales como, dirección IP, máscara de subred y Gateway por defecto.

Se deben preparar además, tablas para cada una de las sedes que documenten las principales características de configuración asignadas a los switches:

**Sede**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nombre Switch** | **Modelo** | **Nº Ptos** | **Piso** | **Dir Ip** | **Gateway** | **VTP Modo** | **STP Raíz** | **Ptos Trunk** | **Ptos VLAN** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

## 3.5 SEGURIDAD DE PUERTO

En cada una de las sedes se debe instalar un servidor http y se desea que la dirección MAC de éste sea considerada la única segura y que cualquier otra, envíe al puerto al modo RESTRICT. Se solicita también que el puerto donde se conectará el servidor no participe en el proceso STP.

## 3.6 DOT1Q Y SUB INTERFACES

La universidad desea que se utilicen sub interfaces en los routers de cada sede para soportar la comunicación entre las diferentes VLANS, por lo que la configuración de los routers debe ajustarse a este requerimiento. En todas las sedes se utilizará la interface FastEthernet 0/0 para tal fin.

# FASE 4 - SEGURIDAD

## 4.1 SEGURIDAD

La universidad desea tener cierto grado de protección, especialmente lo relacionado con el acceso a los servidores ubicados en cada una de las sedes y también desea restringir el uso de ciertos recursos a los usuarios de cada una de las redes. Para la implementación de seguridad se deben tener en cuenta los siguientes aspectos:

* + 1. En la red LAN de servidores de la sede de Bogotá existen los siguientes servidores:
* Un servidor FTP con los archivos fuente de todas las aplicaciones utilizadas en la Universidad. Por ejemplo, instaladores de Windows, Office, aplicativo de contabilidad, etc. Ese servidor está identificado y configurado con la segunda dirección IP disponible en el segmento.
* Un servidor de bases de datos MySQL, identificado y configurado con la tercera dirección IP disponible en el segmento.
* Un servidor HTTP, identificado y configurado con la cuarta dirección IP disponible en el segmento.
* Un servidor TFTP para almacenar las configuraciones y IOS de todos los dispositivos de Red de la institución, identificado y configurado con la quinta dirección IP disponible en el segmento.
  + 1. En las sedes de Pereira y Girardot existe un servidor HTTP identificado con las segundas direcciones IP disponibles en cada segmento.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Servidor** | **Ciudad**  **Ubicación** | **Servicios** | **Dirección IP** | **Puertos** |
| **HTTP** | Girardot | Web | 10.3.160.2 | F0/2 |
| **HTTP** | Pereira | Web | 10.3.192.130 | F0/3 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## 4. 2 ESPECIFICACIONES DE SEGURIDAD

La dirección de la Universidad desea que se implementen las siguientes políticas.

* + 1. El servidor HTTP de la sede Bogotá podrá ser accedido desde cualquier ubicación.
    2. Los servidores HTTP de las sedes de Pereira y Girardot sólo podrán ser vistos por cualquier usuario dentro de la organización.
    3. Los servidores FTP y TFTP de la sede Bogotá sólo podrán ser accedido por los computadores de los administradores de cada sede, que estarán identificados con la siguiente dirección IP disponible en el segmento de Servidores de cada sede.
    4. La universidad cuenta con un proveedor de software, identificado con la dirección IP 200.21.30.31/24 que tendrá acceso al servidor FTP.
    5. A todos los usuarios de la Universidad se les permite el acceso a servicios FTP y HTTP externos.
    6. Al servidor de bases de datos MySQL sólo tendrán acceso los dispositivos ubicados en los segmentos de servidores de cada sede.
    7. El servicio de TELNET estará cerrado para todos, excepto a los dispositivos ubicados los segmentos de servidores.
    8. Ningún usuario de la red interna podrá utilizar los servicios de
    9. Messenger.

# FASE 5 – DHCP

Los routers de cada una de las sedes prestarán los servicios de DHCP para cada uno de los segmentos locales. Dentro de los parámetros de configuración se deben incluir: el nombre de dominio, el Gateway por defeco y el servidor DNS. Se deben excluir del proceso DHCP a las primeras diez direcciones disponibles, las cuales están asignadas a dispositivos de red y son configuradas manualmente.

Se debe diligenciar la siguiente tabla para cada una de las sedes.

Sede \_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nombre del Pool DHCP** | **Dirección de Red / Máscara** | **Direcciones Excluidas** | **Nombre Dominio** | **Gateway por defecto** | **Servidor DNS** |
| **Universidad** | 10.2.0.0/17 | 10.2.0.1-10.2.0.10 | Ucundinamarca.edu.co | 10.2.0.1 | 200.20.30.4 |
| **Bogota-admin** | 10.0.0.0/16 | 10.0.0.1-10.0.0.10 | Ucundinamarca.edu.co | 10.0.0.1 | 200.20.30.4 |
| **Servers-bogota** | 10.3.192.0/25 | 10.3.192.1-10.3.192.10 | Ucundinamarca.edu.co | 10.3.192.1 | 200.20.30.4 |
| **Girardot-administradores** | 10.3.128.0/19 | 10.3.128.1-10.3.128.10 | Ucundinamarca.edu.co | 10.3.128.1 | 200.20.30.4 |
| **Usuarios-girardot** | 10.3.160.0/20 | 10.3.160.1-10.3.160.10 | Ucundinamarca.edu.co | 10.3.160.1 | 200.20.30.4 |
| **Usuarios-pereira** | 10.3.64.0/18 | 10.3.64.1-10.3.64.10 | Ucundinamarca.edu.co | 10.3.64.1 | 200.20.30.4 |
| **Admin-pereira** | 10.2.128.0/17 | 10.2.128.1-10.2.128.10 | Ucundinamarca.edu.co | 10.2.128.1 | 200.20.30.4 |
| **Servers-pereira** | 10.3.192.128/26 | 10.3.192.129-10.3.192.138 | Ucundinamarca.edu.co | 10.3.192.129 | 200.20.30.4 |

# DOCUMENTACIÓN

El caso de estudio debe presentarse de acuerdo con las normas de la Universidad para trabajos escritos y debe contener los siguientes documentos:

1. Archivo en PDF con el desarrollo de las fases propuestas
2. Diagrama de red con el esquema de direccionamiento
3. Archivos de texto plano con la configuración para cada uno de los dispositivos
4. Archivo con la implementación del modelo en el simulador